Customer Copy

Digital Safety

Top Tips

powered by

Digital Eagles

@Digitaleagles

Top Cyber Threats

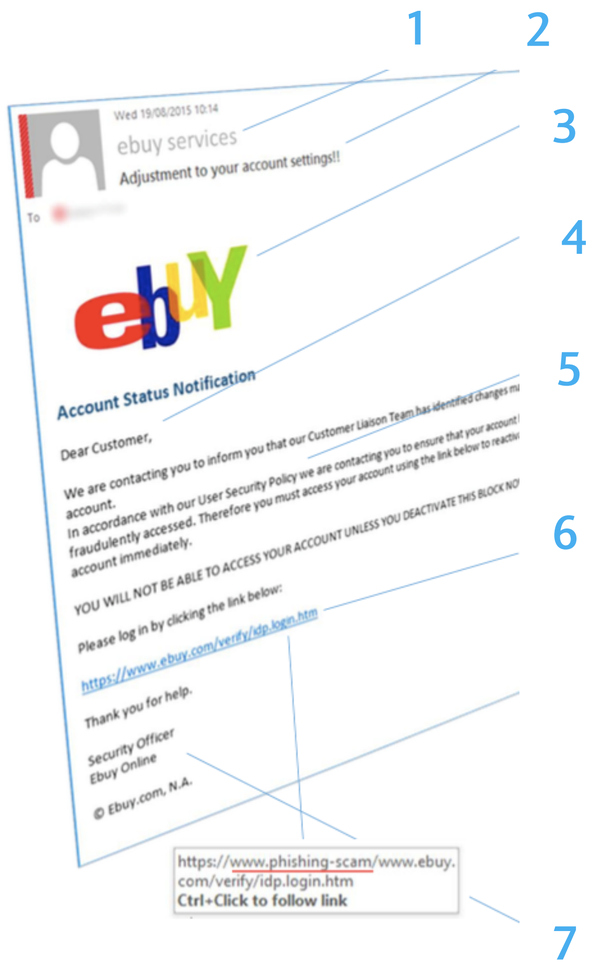
Digital Eagles

Phishing emails

Phishing is a scam where criminals typically send emails to thousands of people. These emails pretend to come from banks, credit card companies, online shops and auction sites as well as other trusted organisations. They usually try to trick you into going to the site, for example to update your password to avoid your account being suspended. The embedded link in the email itself goes to a website that looks exactly like the real thing but is actually a fake designed to trick victims into entering personal information.

- Check and verify the senders email address before opening any attachments from unknown sources.
- Do not click on links in emails from unknown sources - roll your mouse over the link to reveal its true destination.
- Do not respond to emails from unknown sources.
- Do not unsubscribe to what you think may be phishing emails. This may in itself lead to a hoax website.
- Check junk or spam mail folders regularly in case a legitimate email gets through in error.
- Most Microsoft and other email clients come with spam filtering as standard. Ensure yours is switched on.
- Most internet security packages include spam blocking. Ensure that yours is up to date and has this feature switched on.

How to catch a Phish



www.ncsc.gov.uk

1. Sender

Were you expecting this email? Not recognising the sender isn't necessarily cause for concern but look carefully at the sender's name – does it sound legitimate, or is it trying to mimic something you are familiar with?

2. Subject line

Often alarmist, hoping to scare the reader into an action without much thought. May use excessive punctuation.

3. Logo

The logo may be of a low quality if the attacker has simply cut and pasted from a website. Is it even a genuine company?

4. Dear You

Be wary of emails that refer to you by generic names, or in a way you find unusual, such as the first part of your email address. Don't forget though, your actual name may be inferred by your email address.

5. The body

Look out for bad grammar or spelling errors but bear in mind modern phishing looks a lot better than it used to. Many phishing campaigns originate from non-English speaking countries but are written in English in order to target a wider global audience, so word choice may be odd or sound disjointed.

6. The hyperlink/attachment

The whole email is designed to impress on you the importance of clicking this link or attachment right now. For example, if this related to your PayPal account, even if the link to what could be your account looks genuine, hover the mouse over it to reveal the true link. It may provide a clue that this is not a genuine email. If you are still unsure, do not click the link – just open a new webpage and log into your PayPal account via the normal method.

7. Signature block

The signature block may be a generic design or a copy from the real company.

Top Cyber Threats

Digital Eagles

Malicious Software

Malicious software, commonly known as malware, is any software that brings harm to a computer system. Malware can be in the form of worms, viruses, trojans, spyware, adware and rootkits, etc., which steal protected data, delete documents or add software not approved by a user.

Apart from installing internet security software and keeping it updated, we recommend a number of other ways in which to keep your computers, mobile devices and network protected against viruses and spyware.

- Do not open any files attached to an email from an unknown, suspicious or untrustworthy source.
- Be careful with USB connected devices (e.g. memory sticks, external hard drives as they are common carriers of viruses).
- Switch on macro protection in Microsoft Office applications like Word and Excel.
- Buy only reputable software from reputable companies.
- When downloading free software, do so with extreme caution.

Top Cyber Threats

Digital Eagles

Smishing

Smishing – the commonly-used name for SMS phishing – is an activity which enables criminals to steal victims' money or identity, or both as a result of a response to a text message. In common with both phishing, which uses email as an initial approach, and vishing, which uses phone calls, smishing uses your mobile phone (either a smartphone or traditional non-internet connected handset). Like the other methods mentioned, it manipulates innocent people into taking various actions which lead to being defrauded.

How to avoid becoming a victim of smishing

• Do not click on links in text messages unless you are 100% certain that they are genuine and well-intentioned.

• Take time to consider your actions before responding to text messages.

• Ask yourself if the sender, if genuine, would really contact you via this text.

• Recognise threats of financial issues or offers that seem too good to be true, for what they really are.

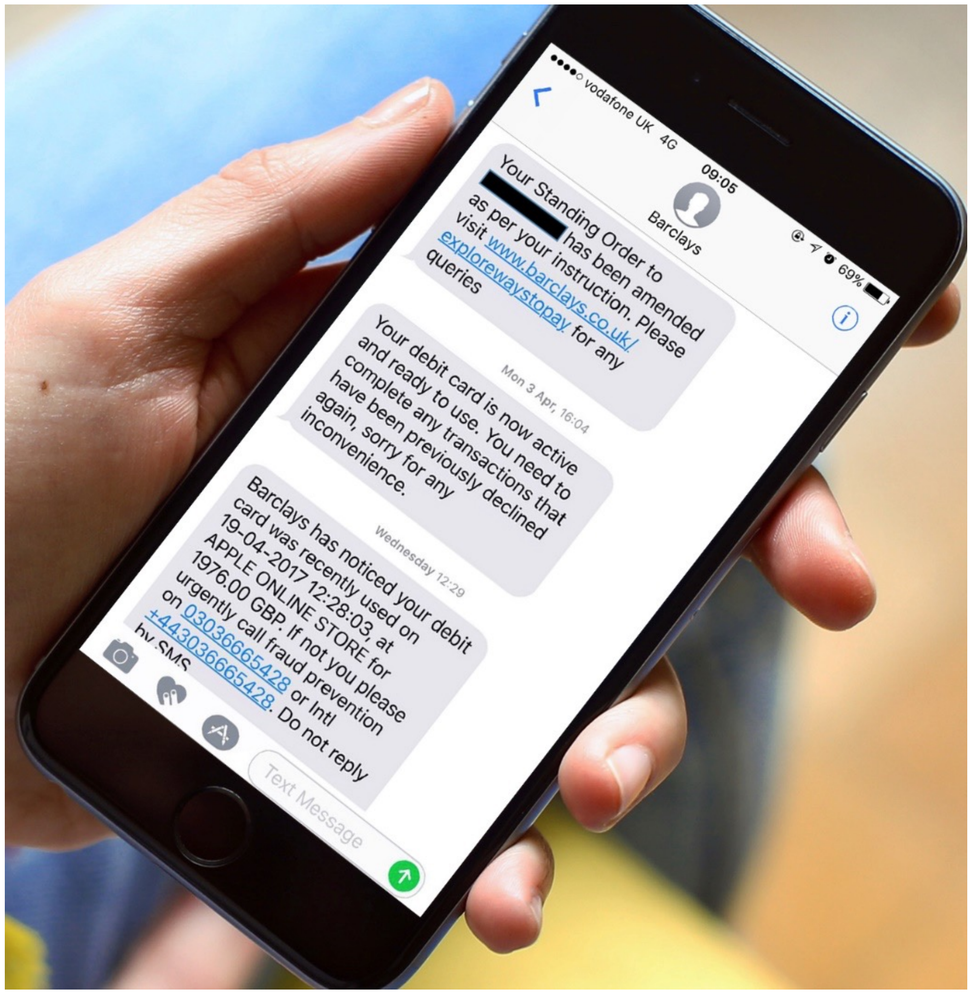
• If in doubt, call the correct number of the organisation or individual from whom the text claims to have been sent, to check its authenticity.

• Remember that even if the text message seems to come from someone you trust, their number may have been hacked or spoofed.

Can you spot the fake text message?

Digital Eagles

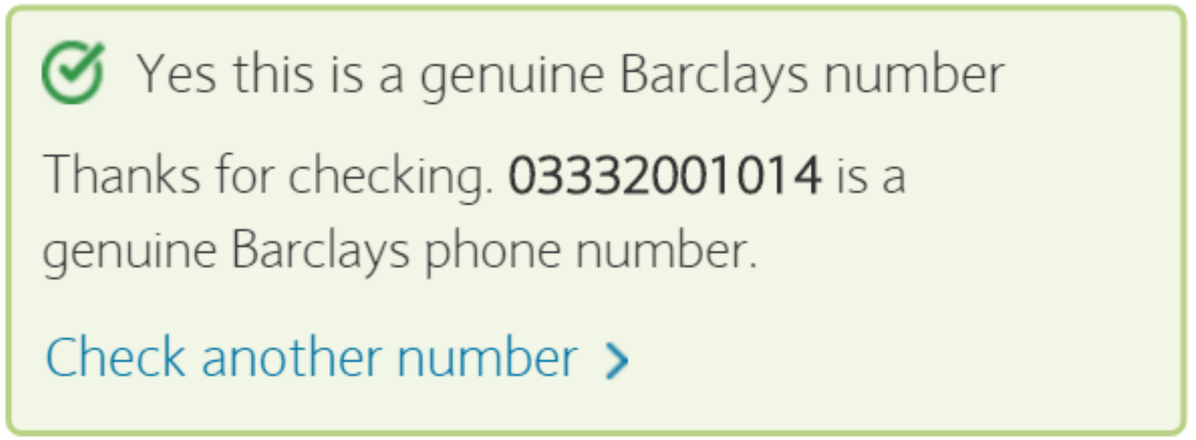
• • • Or • • •



Can you spot the fake text message?

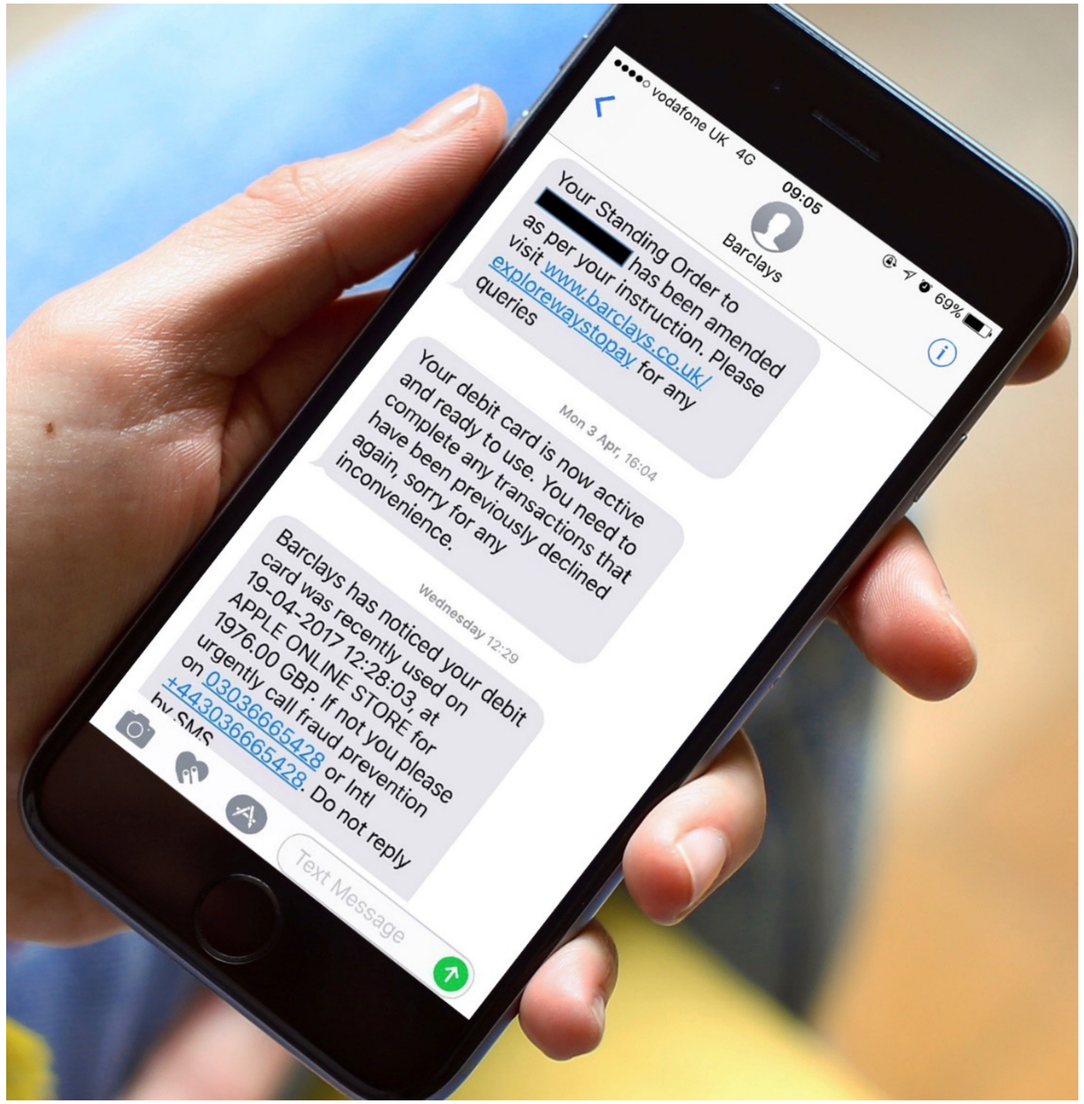
Digital Eagles

The **Barclays Number Checker** is a great way to determine if an SMS is genuine or not.
You can find the number checker on the Barclays Security Page: https://www.barclays.co.uk/security as well as other fantastic articles and a quiz to test your Cyber Security Knowledge.



Can you spot the fake text message?

Digital Eagles



There are other tell-tell signs that this is a scam text as well as checking the phone number on the Barclays Phone Number Checker.
For example, the language used on the APPLE ONLINE STORE Message says “if not you”. Any reputable organisation would use the correct language and grammar, e.g. “if this transaction wasn’t you”.

No this isn’t a genuine Barclays number 03036665428 doesn’t match with a current Barclays phone number. Please check the number you have entered is correct. If you're sure it's the number you've been sent, call us on 0345 734 5345.

Top Cyber Threats

Digital Eagles

Ransomware

Ransomware is a form of malware that gives criminals the ability to lock a computer from a remote location - then displays a pop-up window informing the owner that it will not be unlocked until a sum of money is paid.

Your computer could be infected by ransomware such as CryptoLocker when you inadvertently:

- Open a malicious attachment in an email.
- Click on a malicious link in an email, instant message, social networking site or other website.
- Visit a corrupt website - often these are of a pornographic nature.
- Open infected files from web-based digital file delivery companies (for example Hightail - formerly called YouSendIt, and Dropbox).
- Open corrupt macros in application documents (word processing, spreadsheets etc).
- Connect corrupt USB connected devices (e.g. memory sticks, external hard drives, MP3 players).
- Insert CDs/DVDs that are not from a trusted company into your computer - for example, fraudsters sometimes hand out free ‘music’ CDs/DVDs which are actually corrupted’

Top Cyber Threats

Digital Eagles

Ransomware

Avoiding Ransomware

- Do not reply to, or click on links contained in, unsolicited or spam emails from companies or individuals you do not recognise.
- Visit only websites you know to be reputable.
- Ensure you have effective and updated antivirus/anti-spyware software and firewall running before you go online.
- Regularly back up all your data, including to a USB-connected device stored remotely from your computer. This is because some ransomware can also infect your cloud-based storage.

If you have ransomware on your computer

- To detect and remove ransomware and other malicious software that may be installed on your computer, run a full system scan with an appropriate, up-to-date, security solution.
- If your computer has been locked by ransomware, seek professional advice from a trustworthy source.

Top Cyber Threats

Digital Eagles

Invoice Fraud

- Always verify requests for amended payments to an organisation directly using established contact details

  for example, calling the sender/company on a telephone number that you have previously used to communicate with them.
- If a call seems suspicious, hang up and call the organisation using established contact details.
- Never leave invoices, regular payment mandates or similar information unattended for others to see.
- Check bank statements carefully and report anything suspicious to your bank.

Data Theft

- Control who has access to what data by setting access levels.
- Establish and enforce clear policies about what employees can do with confidential data. Educate the workforce.
- Educate staff on diligence about data access authorisation and email recipient and cc lists.
- Establish a clear BYoD (Bring Your Own Device) policy.
- Encrypt corporate data.

Top Cyber Threats

Digital Eagles

Passwords

Do’s

- Choose a password with at least eight characters (more if you can, as longer passwords are harder for criminals to guess or break), a combination of upper and lower case letters, numbers and keyboard symbols such as @ # $ % ^ & *) _ +. (for example - LqWk&£@240bvURp)

  Also remember that changing letters to numbers (for example E to 3 and i to 1) are techniques well-known to criminals.

- A line of a song that other people would not associate with you.

- Someone else's mother's maiden name (not your own mother's maiden name).

- Pick a phrase known to you, for example 'Tramps like us, baby we were born to run' and take the first character from each word to get 'tlu,bwwbtr'

Top Cyber Threats

Digital Eagles

Passwords

Don’t

Use the following as passwords:

- Your username, actual name or business name.
- Family members’ or pets’ names.
- Your or family birthdays.
- Favourite football or F1 team or other words easy to work out with a little background knowledge.
- Numerical sequences.
- When choosing numerical passcodes or PINs, do not use ascending or descending numbers (for example 4321 or 12345), duplicated numbers (such as 1111) or easily recognisable keypad patterns (such as 14789 or 2580).

Are you using…

Digital Eagles

Two-step authentication

Two-step authentication is a security measure designed to stop website breaches or theft of personal information. This extra level of security helps to lessen the risk of your Facebook account, or banking details, being accessed by someone who wants to exploit your digital identity.

A two-step authentication system – whether it's via a passcode generator for your bank account or a code sent to you phone via text message – works by adding a second password to protected accounts that, theoretically, only you will have access to.

The following companies support two-step authentication; Apple, Facebook, Twitter, LinkedIn, Google, Microsoft, PayPal, WordPress. You can check a full list of those companies who support this service at https://twofactorauth.org

Social Engineering

Digital Eagles

- Never reveal confidential or financial company or customer data including usernames, passwords, PINs, or ID numbers.
- Be very careful that people or organisations to whom you are supplying payment card information are genuine, and then never reveal passwords. Remember that a bank or other reputable organisation will never ask you for your password via email or phone call.
- If you receive a phone call requesting confidential information, we strongly recommend that you ask for a full and correct spelling of the caller's name and/or company, **hang up and search on the trusted company's website for a contact number to ring back on.**

Google

1 9 2 .com
People, Businesses & Places

WIKIPEDIA
The Free Encyclopedia

Social Engineering

Digital Eagles

- If you are asked by a caller to cut off the call and phone your bank or card provider, call the number on your bank statement or other document from your bank – or on the back of your card – but be sure to use another phone from the one you received the call on. If you cannot access another phone, be sure to hang up for at least five minutes before you dial out, or call a friend (whose voice you recognise) before making another call.
- Never open email attachments from unknown sources.

Source: https://www.getsafeonline.org

Google

1 9 2 .com
People, Businesses & Places

WIKIPEDIA
The Free Encyclopedia

Ways to protect you, your family and your business

Internet Security Software

Digital Eagles

- It is vital to keep your internet security software up to date in order to provide the most complete protection.
- Thousands of new viruses are detected every day, each has a set of characteristics or ‘signatures’ that enable internet security software manufacturers to detect them and produce suitable updates.
- You will generally receive a notification from the software manufacturer in the form of an alert on your screen, that updates are available.
- You will normally be given the choice of whether to download and install the update immediately or later. Our recommendation is to download and install as soon as possible.

Data Backup

Digital Eagles

- Two principal methods of backup are available. To choose which to use, you need to consider capacity required, ease of use, speed, price and integrity.

- External hard disks are a fast, efficient way of backing up your data. Models are available that either plug into your computer's USB port, or connect via your wireless network. Most are sufficiently compact that they can easily be stored off-site to facilitate off-site storage.

- The use of online backup (also known as 'cloud backup') is becoming commonplace owing to its added convenience, security and low cost.

- There is virtually no limit to the volume of data that can be backed up in the cloud. Some providers supply limited storage free of charge, but generally the cost of backups increases proportionally to the amount of data involved.

Digital Eagles

Public Wi-Fi

- Cyber criminals often spy on public Wi-Fi networks and intercept data that is transferred across the link.
- The criminal can access users' banking credentials, account passwords, and other valuable information.
- Don't just assume that the Wi-Fi link is legitimate.
- It could be a bogus link that has been set up by a cybercriminal that's trying to capture valuable, personal information from unsuspecting users.

Smartphone Security

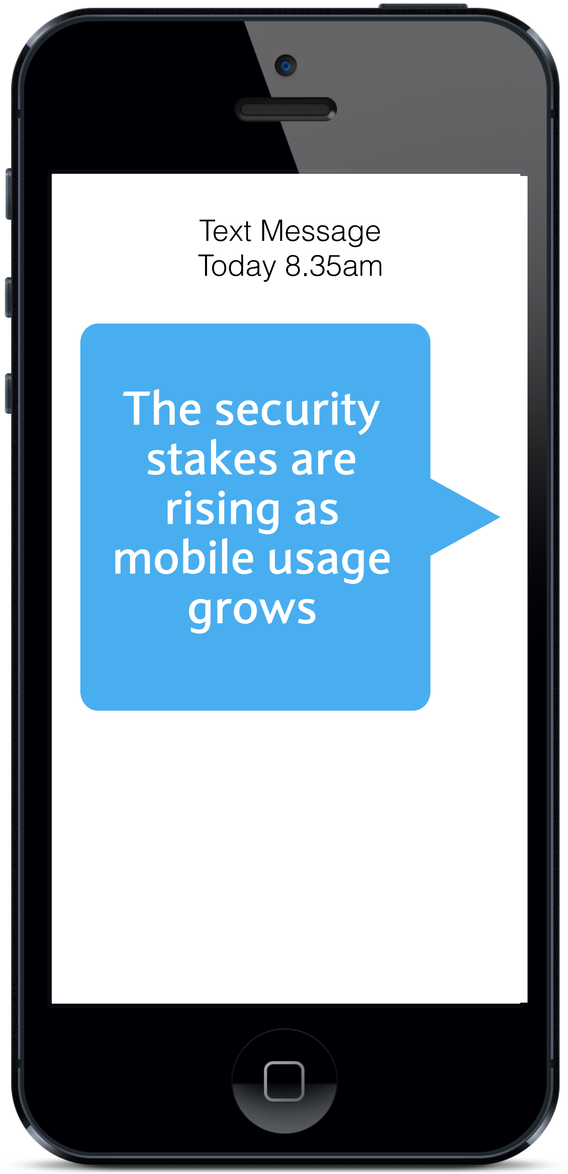
Activate a screen lock - your phone should auto lock itself after a short period)

Use a password to unlock the screen - Biometrics are one of the most secure ways to authenticate)

Be careful with those apps - You could be exposed to Malware / adware / ransomware. Only download from official app stores.

Watch out what you click on - don't click on links that you didn't request

Activate automatic backup in the cloud - in case your phone is destroyed, lost or stolen



Basic security settings for smartphones can be tweaked by anyone

Prevention

Digital Eagles

Make sure your Passwords are secure

Regularly update your Security Software

Always keep your data backed up securely

Prevention

Digital Eagles

Check the source of your email

Ensure the website is secure

Think before you click the link

Road to Recovery

Digital Eagles

- If you are a victim of cyber crime or fraud and have suffered a financial loss, you should contact your bank immediately. If you alert your bank as soon as possible you may be able to recover any lost funds.

- Action Fraud is the UK's national fraud and cyber crime reporting centre. Visit actionfraud.police.uk to report fraud, attempted fraud or cyber crime using the online fraud reporting tool and receive a police crime reference number.

- Alternatively you can speak to a specialist fraud advisor at Action Fraud on 0300 123 2040.

- Contact your local police who can also provide crime prevention advice and support.

POLICE

ActionFraud

Report Fraud & Internet Crime

actionfraud.police.uk

Useful resources

Digital Eagles

CYBER AWARE

Digital Wings
Created by BARCLAYS

GET SAFE ONLINE .org

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

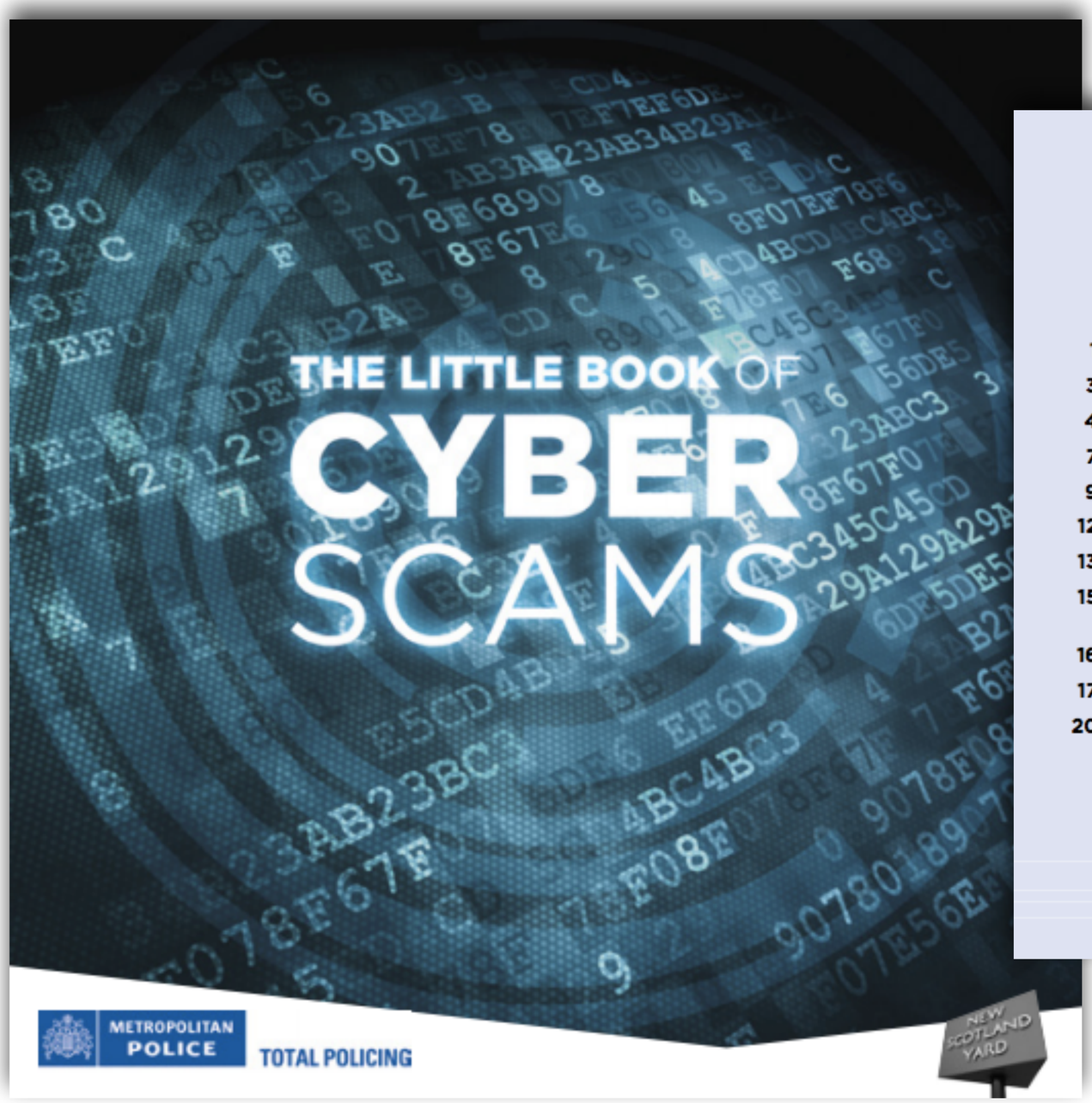
TAKE FIVE TO STOP FRAUD™

POLICE

FFA
Financial Fraud Action UK
Working together to prevent fraud

CYBER ESSENTIALS

Digital Eagles



CONTENTS

METROPOLITAN POLICE

Notes…but no passwords!

Digital Eagles